20220207.1008610

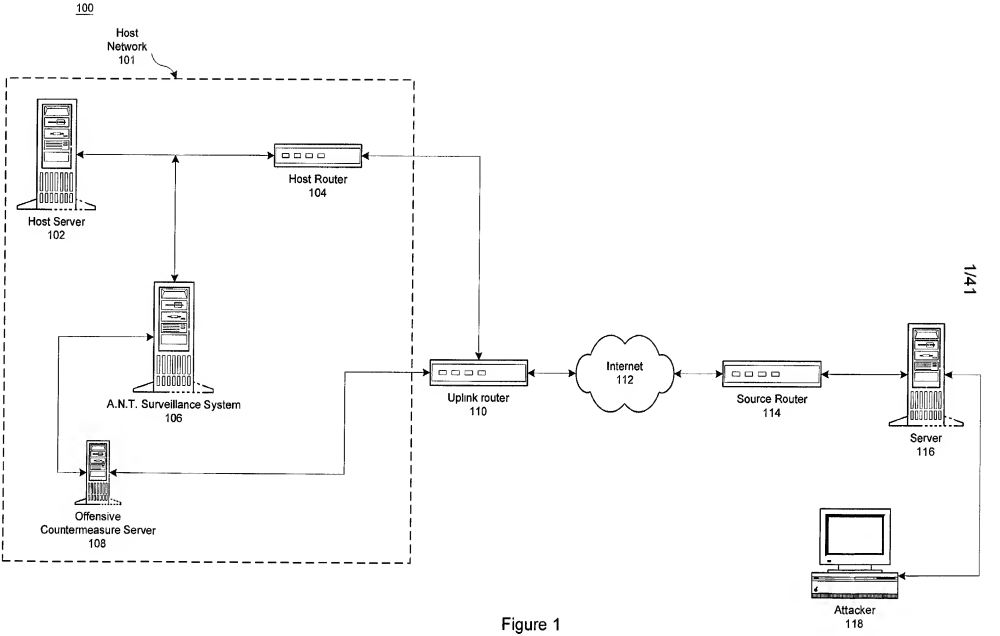

Figure 1

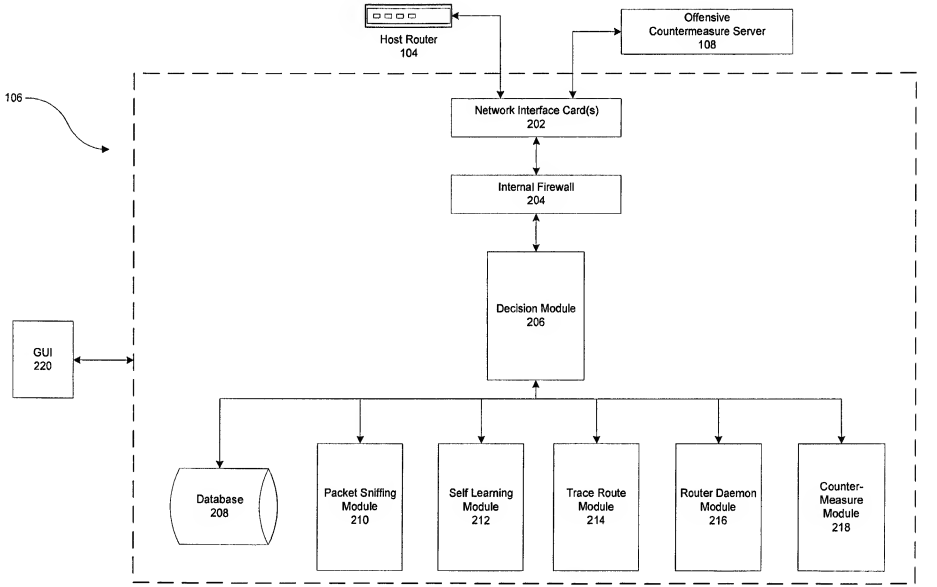
Host Router
104
Offensive
Countermeasure Server
108
106
Network Interface Card(s)
202
Internal Firewall
204
Decision Module
206
GUI
220
Database
208
Packet Sniffing
Module
210
Self Learning
Module
212
Trace Route
Module
214
Router Daemon
Module
216
Counter-
Measure
Module
218

Figure 2

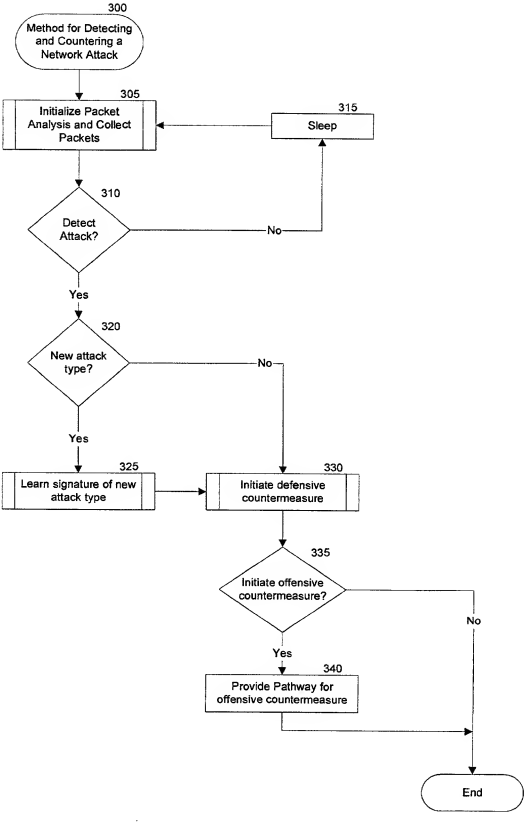

Figure 3

2008220'A1'US 20080301

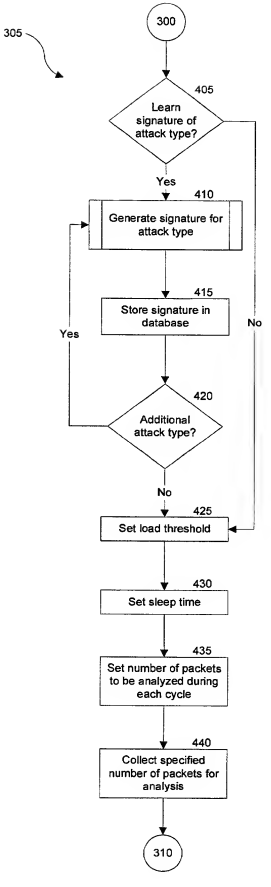

Figure 4

2003220 / 2003900001

10085107-022802

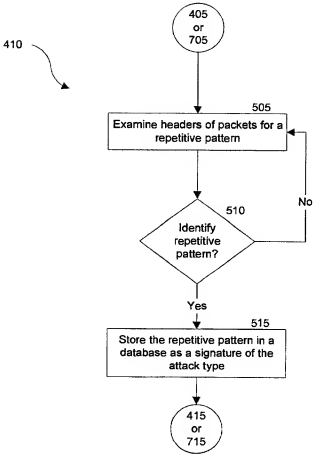

Figure 5

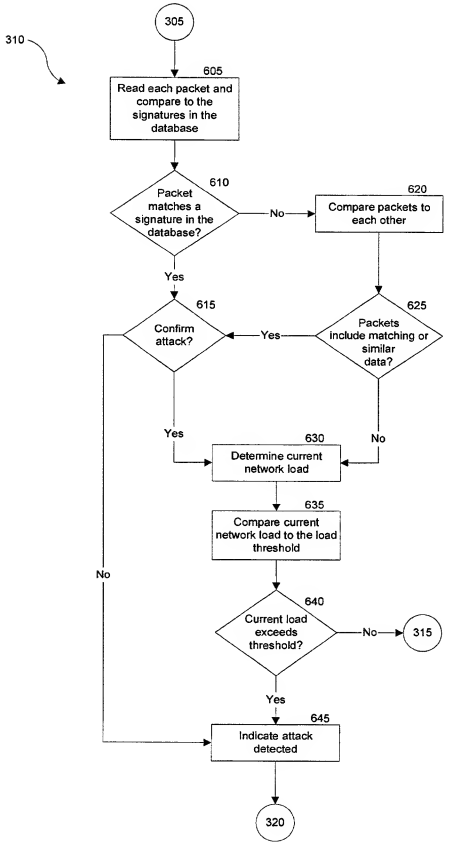

Figure 6

10085107.022801

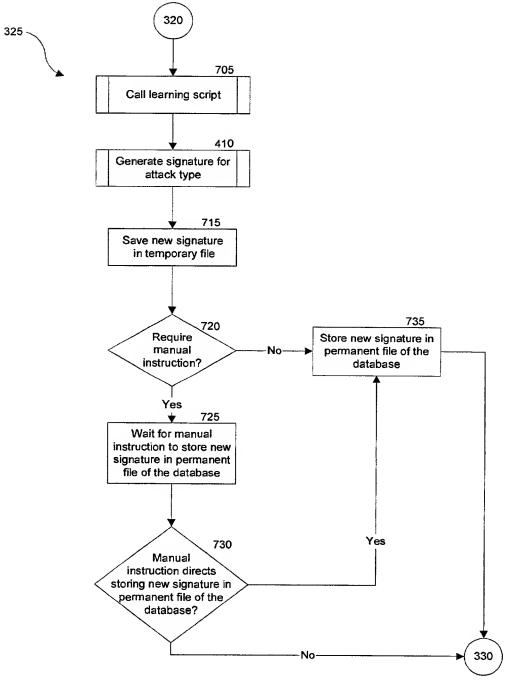

Figure 7

2008220 "2007/098001

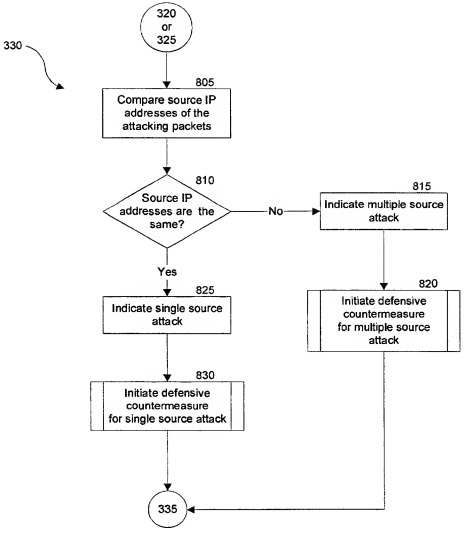

Figure 8

20020147930021

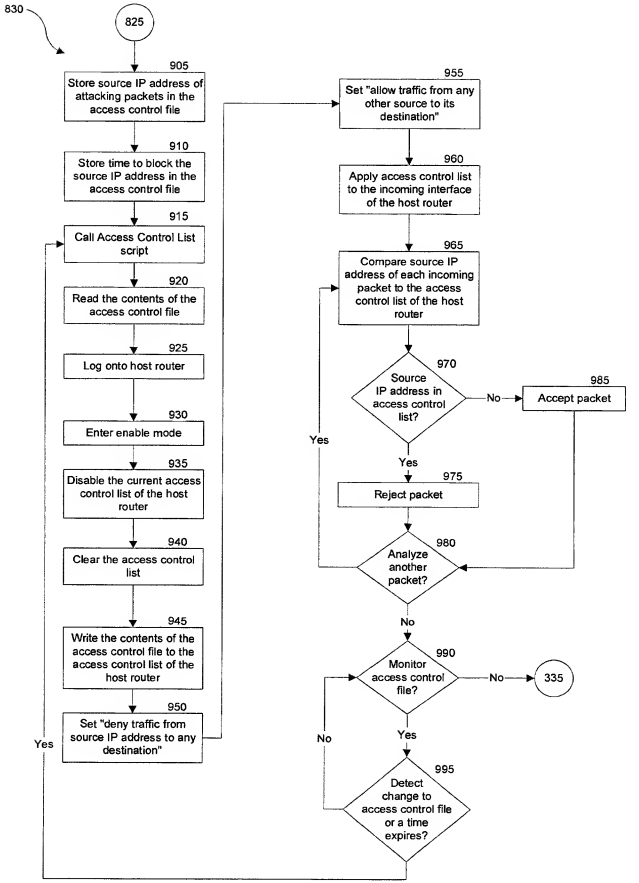

Figure 9

20080107-022802

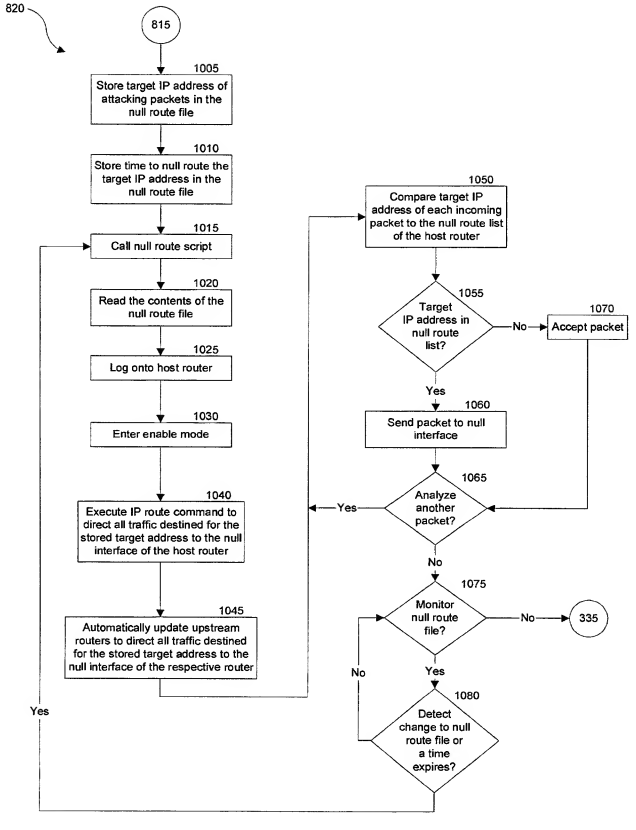
820
815
1005
Store target IP address of attacking packets in the null route file
1010
Store time to null route the target IP address in the null route file
1015
Call null route script
1020
Read the contents of the null route file
1025
Log onto host router
1030
Enter enable mode
1040
Execute IP route command to direct all traffic destined for the stored target address to the null interface of the host router
1045
Automatically update upstream routers to direct all traffic destined for the stored target address to the null interface of the respective router
Yes
1050
Compare target IP address of each incoming packet to the null route list of the host router
1055
Target IP address in null route list?
No
1070
Accept packet
Yes
1060
Send packet to null interface
1065
Analyze another packet?
Yes
No
1075
Monitor null route file?
No
335
No
Yes
1080
Detect change to null route file or a time expires?

Figure 10

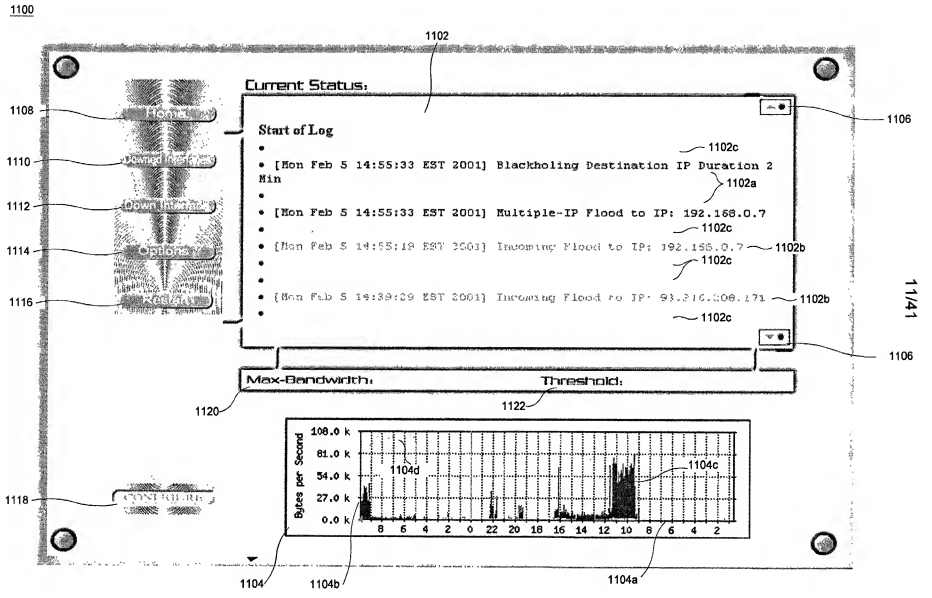
1100
1102
Current Status:
Start of Log
[Mon Feb 5 14:55:33 EST 2001] Blackholing Destination IP Duration 2 Min
[Mon Feb 5 14:55:33 EST 2001] Multiple-IP Flood to IP: 192.168.0.7
[Mon Feb 5 14:55:18 EST 2001] Incoming Flood to IP: 192.168.0.7
[Mon Feb 5 14:39:29 EST 2001] Incoming Flood to IP: 63.216.208.171
1102a
1102b
1102c
1106
Max-Bandwidth:
Threshold:
1120
1122
108.0 k
81.0 k
54.0 k
27.0 k
0.0 k
Bytes per Second
8 6 4 2 0 22 20 18 16 14 12 10 8 6 4 2
1104
1104a
1104b
1104c
1104d
1108
1110
1112
1114
1116
1118

Figure 11

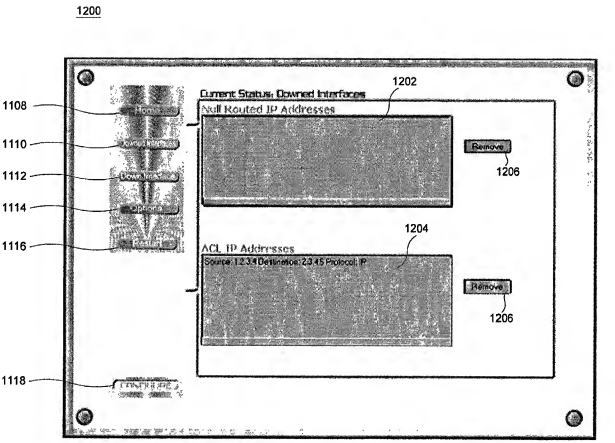
1200
1202
Current Status: Downed Interfaces
Null Routed IP Addresses
Remove
1206
1204
ACL IP Addresses
Source 1.2.3.4 Destination 2.3.4.5 Protocol: IP
Remove
1206
1108
1110
1112
1114
1116
1118

Figure 12

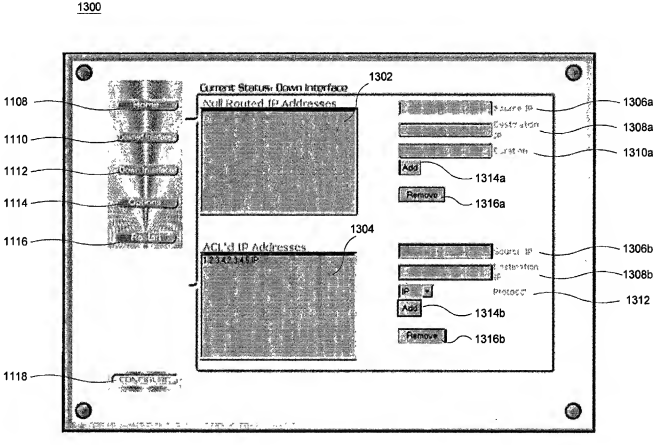
1300
1108
1110
1112
1114
1116
1118
1302
Current Status: Down Interface
Null Routed IP Addresses
1304
ACL'd IP Addresses
1306a
1308a
1310a
1314a
1316a
1306b
1308b
1312
1314b
1316b
Add
Remove
IP
Protocol

Figure 13

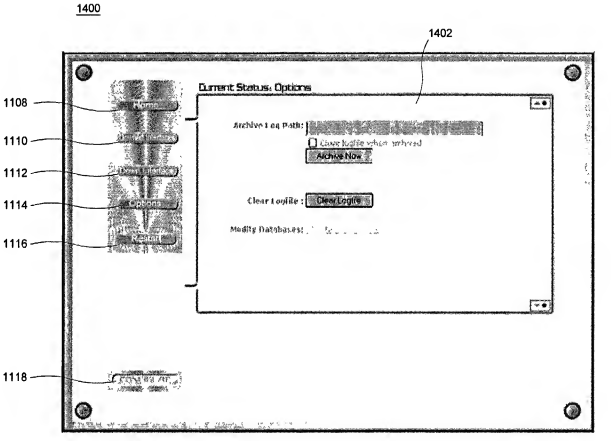
1400
1402
1108
1110
1112
1114
1116
1118
Current Status, Options
Archive Log Path:
Archive Now
Clear Logfile :
Clear Logfile
Modify Database:

Figure 14

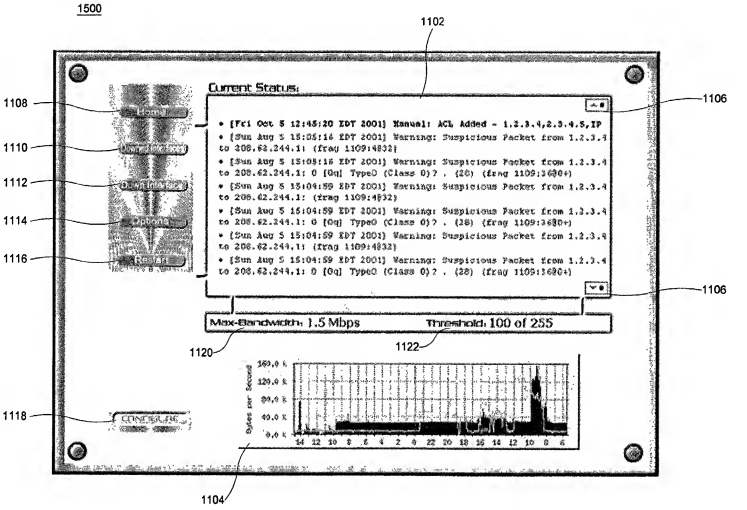
1500
1102
1108
1110
1112
1114
1116
1106
1106
1120
1122
1118
1104
Current Status:
Max-Bandwidth: 1.5 Mbps
Threshold: 100 of 255
Bytes per Second

Figure 15

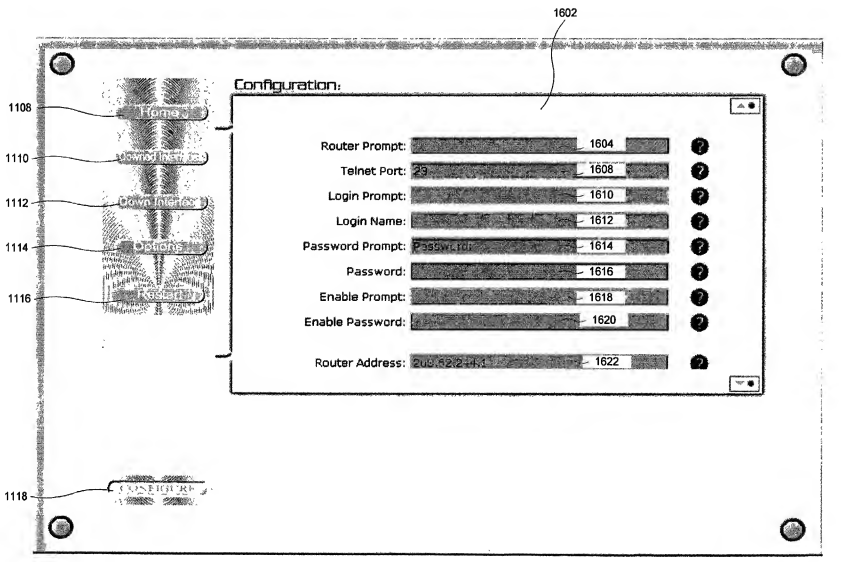
1600
1602
Configuration:
1108
Transmit
1110
Download Interfaces
1112
Down Interface
1114
Options
1116
Select Port
1118
Configure
Router Prompt:
1604
Telnet Port:
29
1608
Login Prompt:
1610
Login Name:
1612
Password Prompt:
Password
1614
Password:
1616
Enable Prompt:
1618
Enable Password:
1620
Router Address:
1622

Figure 16A

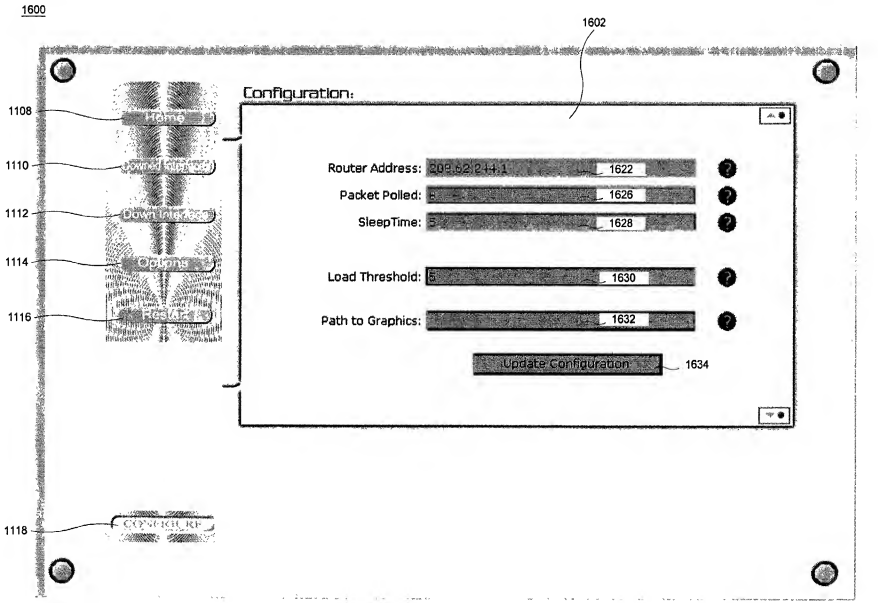
1600
1602
Configuration:
1108
Home
1110
Download Files
1112
Download Files
1114
Options
1116
1118
Router Address:
1622
Packet Polled:
1626
SleepTime:
1628
Load Threshold:
1630
Path to Graphics:
1632
Update Configuration
1634

Figure 16B

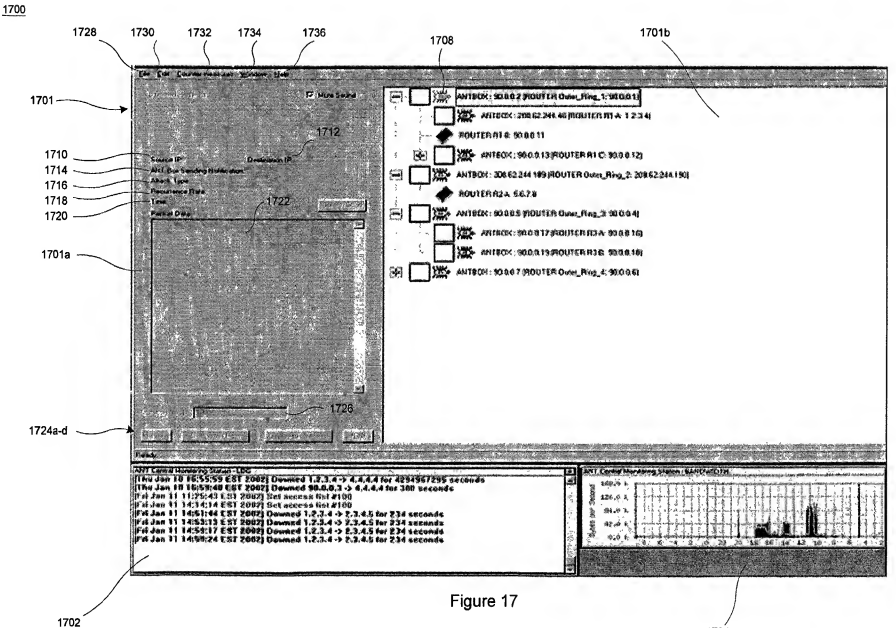
1700
1728
1730
1732
1734
1736
1708
1701b
1701
1712
1710
1714
1716
1718
1720
1722
1701a
1726
1724a-d
1702
1704

Figure 17

2008220"07198001

Figure 18

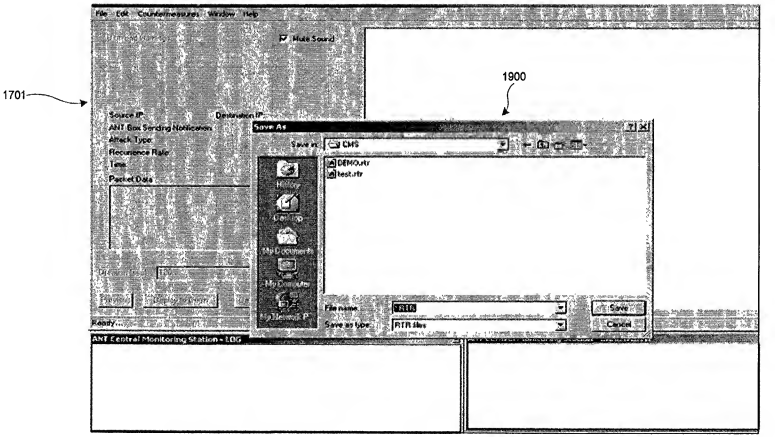
1701
1900
Mute Sound
Source IP:
Destination IP:
ANT Box Sending Notification
Attack Type:
Recurrence Rate:
Time:
Packet Data
Save As
Save in:
CMS
DEMOuttr
testLittr
Filename:
*.RTR
Save as type:
RTR files
Save
Cancel
ANT Central Monitoring Station - LOG

Figure 19

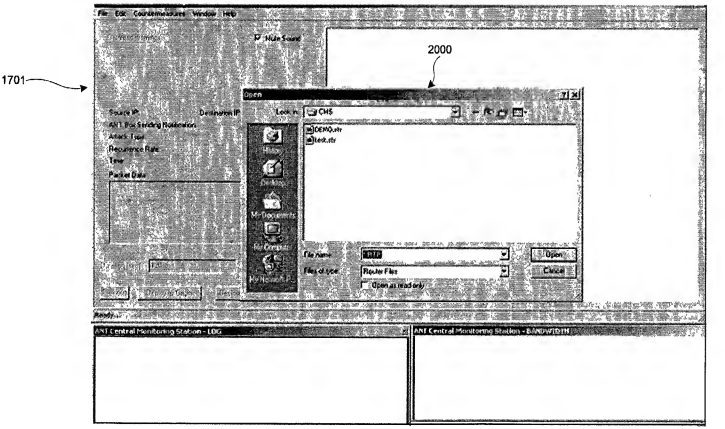
1701
2000
File Edit Countermeasures Window Help
Mute Sound
Open
Look In:
CMS
DEMO.stv
test.stv
File Name:
*.STD
Open
Files of type:
Router Files
Cancel
Open as read-only
Ready
ANT Central Monitoring Station - LOG
ANT Central Monitoring Station - BANDWIDTH

Figure 20

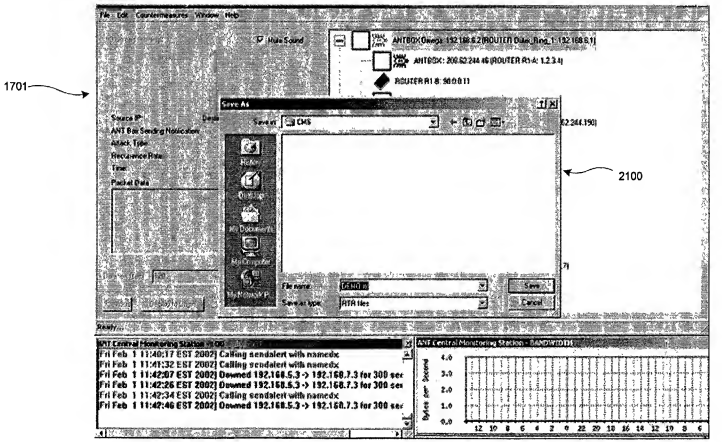
1701
2100
Save As
Save in:
CMS
File name:
Save as type:
RTA files
Save
Cancel
Ready
Fri Feb 1 11:40:17 EST 2002] Calling sendalert with namedx
Fri Feb 1 11:41:32 EST 2002] Calling sendalert with namedx
Fri Feb 1 11:42:07 EST 2002] Downed 192.168.5.3 -> 192.168.7.3 for 300 sec
Fri Feb 1 11:42:26 EST 2002] Downed 192.168.5.3 -> 192.168.7.3 for 300 sec
Fri Feb 1 11:42:34 EST 2002] Calling sendalert with namedx
Fri Feb 1 11:42:46 EST 2002] Downed 192.168.5.3 -> 192.168.7.3 for 300 sec
ANT Central Monitoring Station - BANDWIDTH
Bytes per Second
4.0
3.0
2.0
1.0
0.0

Figure 21

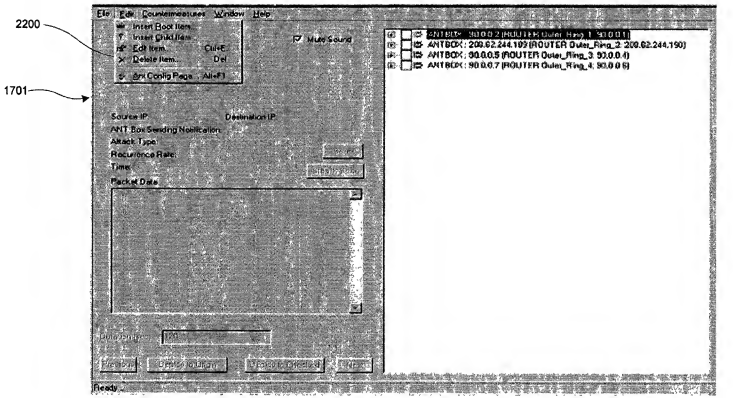
2200
1701
File Edit Countermeasures Window Help
Insert Root Item...
Insert Child Item...
Edit Item... Ctrl+E
Delete Item... Del
Set Config Page... Alt+F1
Mute Sound
ANTBOX: 90.0.0.2 (ROUTER Outer_Ring_1: 90.0.0.1)
ANTBOX: 209.62.244.109 (ROUTER Outer_Ring_2: 209.62.244.190)
ANTBOX: 90.0.0.5 (ROUTER Outer_Ring_3: 90.0.0.4)
ANTBOX: 90.0.0.7 (ROUTER Outer_Ring_4: 90.0.0.6)
Source IP
Destination IP
ANT Box Sending Notification
Attack Type
Recurrence Rate:
Time:
Packet Data
Ready

Figure 22

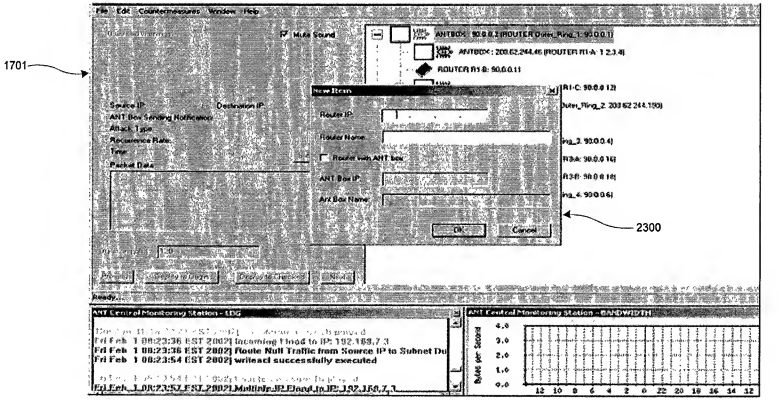
1701
2300
File Edit Countermeasures Window Help
RF Mute Sound
ANTBOX: 90.0.0.1 (ROUTER Outer_Ring_1: 90.0.0.1)
ANTBOX: 200.62.244.46 (ROUTER R1-A: 1.2.3.4)
ROUTER R1-B: 90.0.0.11
New Items
Router IP:
Router Name:
Router with ANT box
ANT Box IP:
Ant Box Name:
OK
Cancel
Source IP:
Destination IP:
ANT Box Sending Notification:
Attack Type:
Occurrence Rate:
Time:
Packet Data:
ANT Central Monitoring Station - LOG
Fri Feb 1 08:23:36 EST 2002] Incoming Flood to IP: 192.168.7.3
Fri Feb 1 08:23:36 EST 2002] Route Null Traffic from Source IP to Subnet Du
Fri Feb 1 08:23:54 EST 2002] wrlead successfully executed
ANT Central Monitoring Station - BANDWIDTH
Bytes per Second
4.0
3.0
2.0
1.0
0.0
12 10 8 6 4 2 0 22 20 18 16 14 12

Figure 23

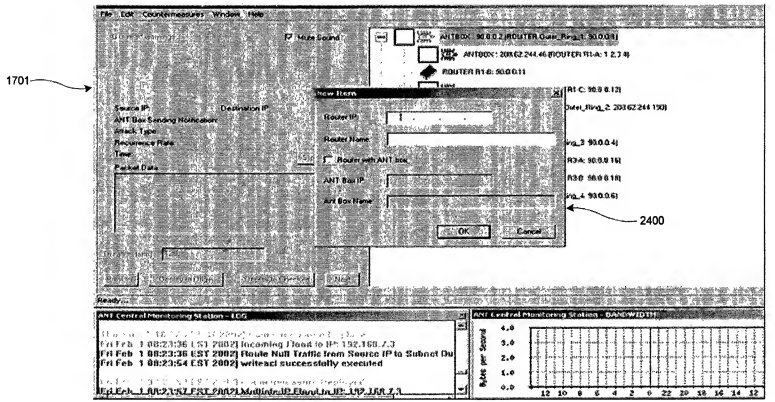
1701
2400
File Edit Countermeasures Windows Help
Mute Sound
New Item
Router IP
Router Name
Router with ANT box
ANT Box IP
Ant Box Name
OK
Cancel
Source IP
Destination IP
ANT Box Sending Notification
Attack Type
Frequence Rate
Time
Packet Data
Ready...
ANT Central Monitoring Station - LOG
Fri Feb 1 08:23:36 EST 2002] Incoming flood to IP: 192.168.7.3
Fri Feb 1 08:23:36 EST 2002] Route Null Traffic from Source IP to Subnet Du
Fri Feb 1 08:23:54 EST 2002] writeacl successfully executed
ANT Central Monitoring Station - BANDWIDTH
Byte per Second
4.0
3.0
2.0
1.0
0.0
12 10 8 6 4 2 0 22 20 18 16 14 12

Figure 24

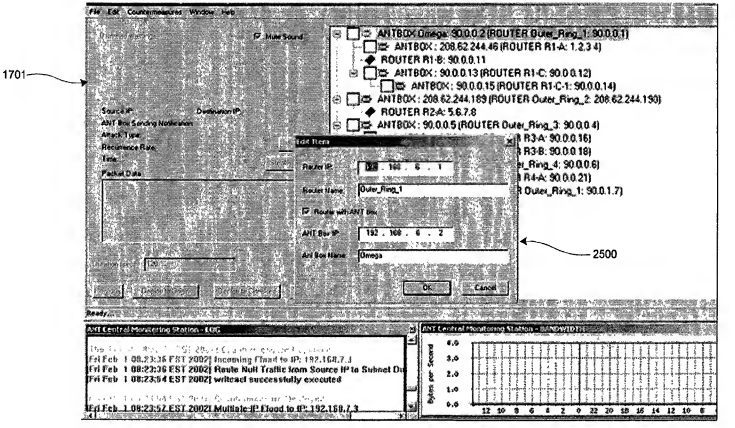
1701
2500
ANTBOX Omega: 90.0.0.2 (ROUTER Outer_Ring_1: 90.0.0.1)
ANTBOX : 208.62.244.46 (ROUTER R1-A: 1.2.3.4)
ROUTER R1-B: 90.0.0.11
ANTBOX : 90.0.0.13 (ROUTER R1-C: 90.0.0.12)
ANTBOX: 90.0.0.15 (ROUTER R1-C-1: 90.0.0.14)
ANTBOX : 208.62.244.169 (ROUTER Outer_Ring_2: 208.62.244.190)
ROUTER R2-A: 5.6.7.8
ANTBOX : 90.0.0.5 (ROUTER Outer_Ring_3: 90.0.0.4)
R3-A: 90.0.0.16)
R3-B: 90.0.0.18)
R_Ring_4: 90.0.0.6)
R4-A: 90.0.0.21)
Outer_Ring_1: 90.0.1.7)
Edit Item
Router IP
Router Name
Outer_Ring_1
Route with ANT Box
ANT Box IP
ANT Box Name
Omega
OK
Cancel
ANT Central Monitoring Station - LOG
Fri Feb 1 08:23:36 EST 2002] Incoming Flood to IP: 192.168.7.1
Fri Feb 1 08:22:36 EST 2002] Route Null Traffic from Source IP to Subnet Da
Fri Feb 1 08:23:54 EST 2002] writeacl successfully executed
Fri Feb 1 08:23:57 EST 2002] Multiple IP Flood to IP: 192.168.7.3
ANT Central Monitoring Station - BANDWIDTH
Bytes per Second
6.0
5.0
4.0
3.0
2.0
1.0
0.0

Figure 25

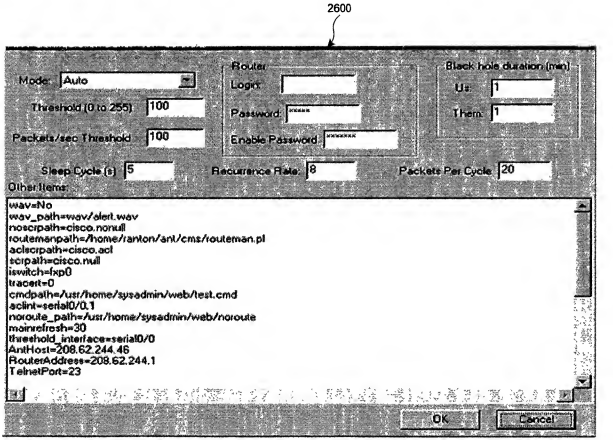
2600
Mode: Auto
Threshold (0 to 255) 100
Packets/sec Threshold 100
Router
Login:
Password: *****
Enable Password: *******
Black hole duration (min)
Us: 1
Them: 1
Sleep Cycle (s) 5
Recurrence Rate: 8
Packets Per Cycle: 20
Other Items:
wav=No
wav_path=wav/alert.wav
noscript=cisco.nonull
routemanpath=/home/ranton/ant/cms/routeman.pl
aclscript=cisco.acl
script=cisco.null
iswitch=fxp0
tracert=0
cmdpath=/usr/home/sysadmin/web/test.cmd
aclint=serial0/0.1
noroute_path=/usr/home/sysadmin/web/noroute
mainrefresh=30
threshold_interface=serial0/0
AntHost=208.62.244.46
RouterAddress=208.62.244.1
TelnetPort=23
OK
Cancel

Figure 26

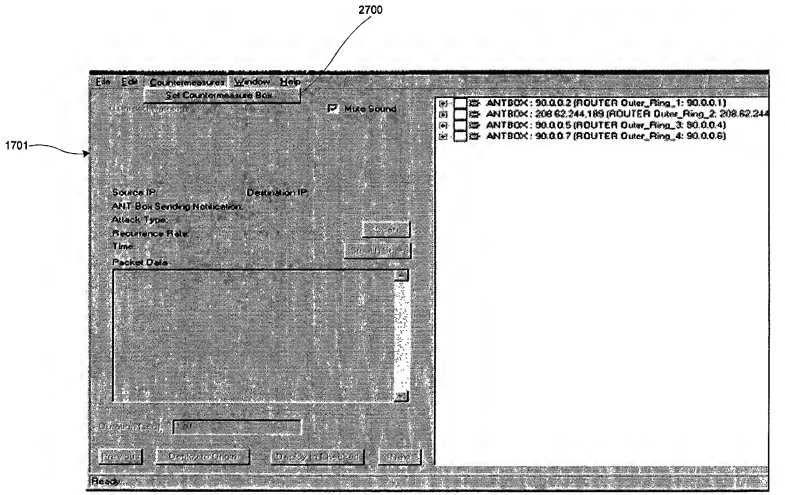
2700
1701
File Edit Countermeasures Window Help
Set Countermeasure Box...
Mute Sound
ANTBOX: 90.0.0.2 (ROUTER Outer_Ring_1: 90.0.0.1)
ANTBOX: 208.62.244.189 (ROUTER Outer_Ring_2: 208.62.244
ANTBOX: 90.0.0.5 (ROUTER Outer_Ring_3: 90.0.0.4)
ANTBOX: 90.0.0.7 (ROUTER Outer_Ring_4: 90.0.0.6)
Source IP:
Destination IP:
ANT Box Sending Notification:
Attack Type:
Recurrence Rate:
Time:
Packet Data:
Ready...

Figure 27

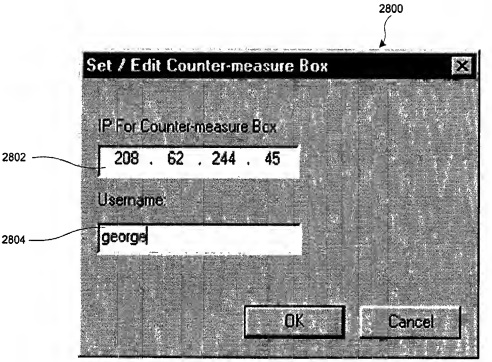
2800
Set / Edit Counter-measure Box
IP For Counter-measure Box
2802
208 . 62 . 244 . 45
Username:
2804
george
OK
Cancel

Figure 28

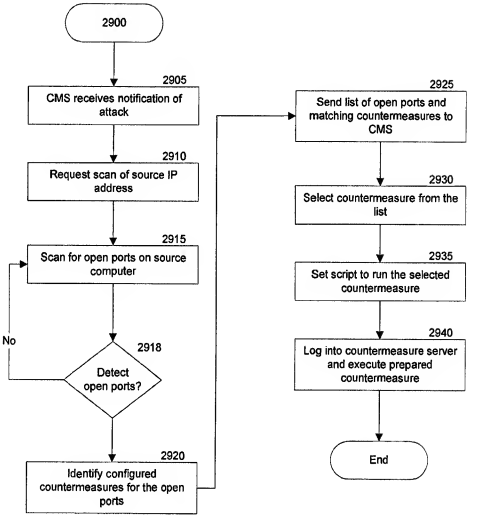
2900
2905
CMS receives notification of attack
2910
Request scan of source IP address
2915
Scan for open ports on source computer
No
2918
Detect open ports?
2920
Identify configured countermeasures for the open ports
2925
Send list of open ports and matching countermeasures to CMS
2930
Select countermeasure from the list
2935
Set script to run the selected countermeasure
2940
Log into countermeasure server and execute prepared countermeasure
End

Figure 29

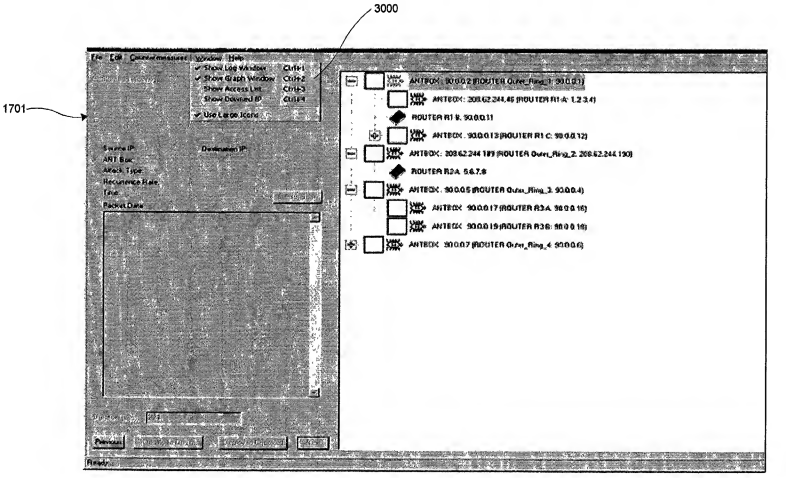
3000
1701
Show Log Window Ctrl+1
Show Graph Window Ctrl+2
Show Access List Ctrl+3
Show Denied IP Ctrl+4
Use Large Icons
Source IP
Destination IP
ART Box
Attack Type
Recurrence Rate
Time
Packet Data
ROUTER R1 B. 90.0.0.11
ROUTER R2A 5.6.7.8

Figure 30

2008220.2007810.1

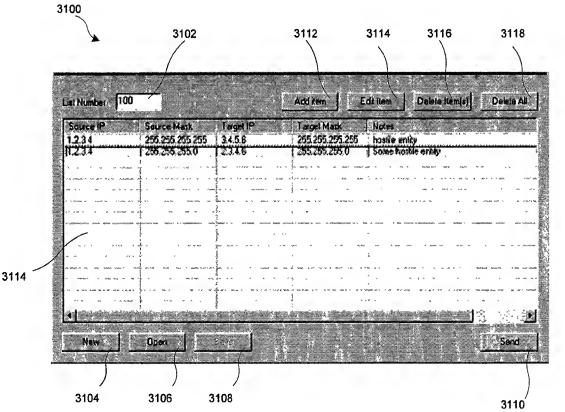

Figure 31

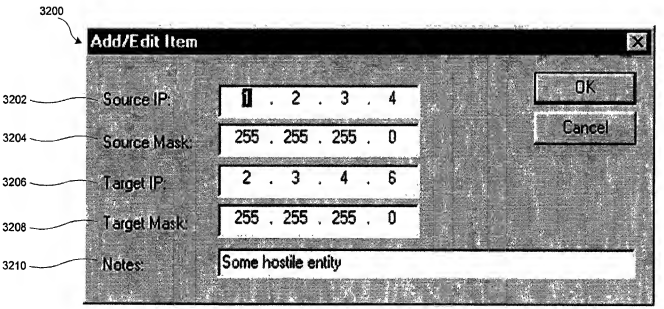
3200
Add/Edit Item
OK
Cancel
3202
Source IP:
1 . 2 . 3 . 4
3204
Source Mask:
255 . 255 . 255 . 0
3206
Target IP:
2 . 3 . 4 . 6
3208
Target Mask:
255 . 255 . 255 . 0
3210
Notes:
Some hostile entity

Figure 32

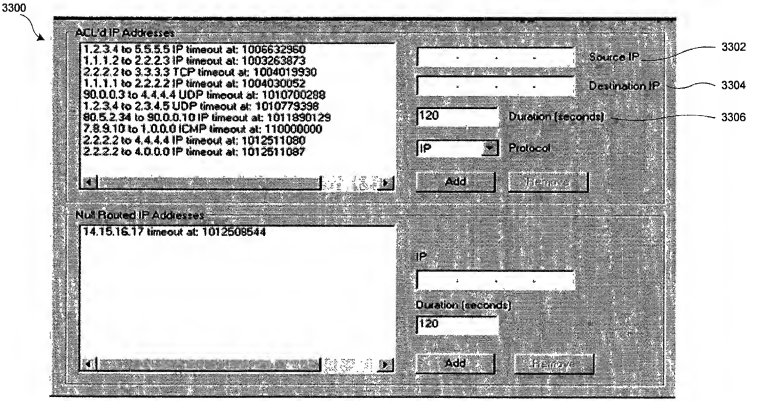
3300
ACL'd IP Addresses
1.2.3.4 to 5.5.5.5 IP timeout at: 1006632960
1.1.1.2 to 2.2.2.3 IP timeout at: 1003263873
2.2.2.2 to 3.3.3.3 TCP timeout at: 1004019930
1.1.1.1 to 2.2.2.2 IP timeout at: 1004030052
90.0.0.3 to 4.4.4.4 UDP timeout at: 1010700288
1.2.3.4 to 2.3.4.5 UDP timeout at: 1010779398
80.5.2.34 to 90.0.0.10 IP timeout at: 1011890129
7.8.9.10 to 1.0.0.0 ICMP timeout at: 110000000
2.2.2.2 to 4.4.4.4 IP timeout at: 1012511080
2.2.2.2 to 4.0.0.0 IP timeout at: 1012511087
Source IP
Destination IP
120
Duration (seconds)
IP
Protocol
Add
Remove
Null Routed IP Addresses
14.15.16.17 timeout at: 1012508544
IP
Duration (seconds)
120
Add
Remove
3302
3304
3306

Figure 33

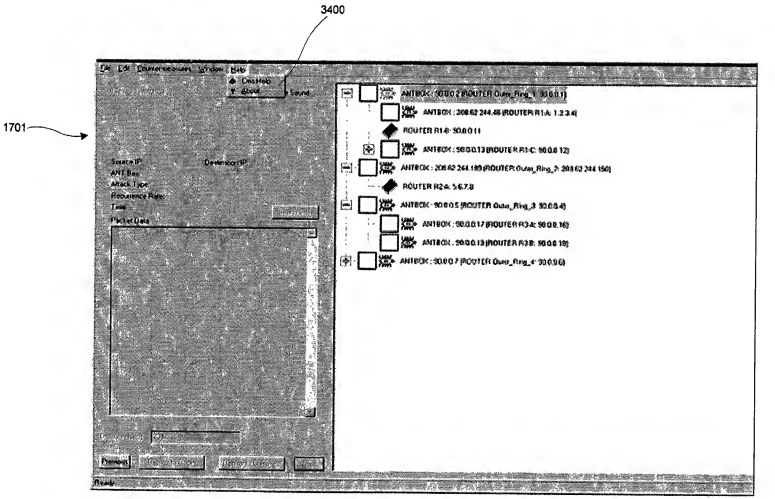
3400
1701
Source IP
Destination IP
ANT Bot
Attack Type
Frequence Rate
Time
Packet Data
ANTBOX : 208.62.244.46 (ROUTER R1A: 1.2.3.4)
ROUTER R1A: 50.0.0.11
ROUTER R2A: 5.6.7.8
Ready

Figure 34

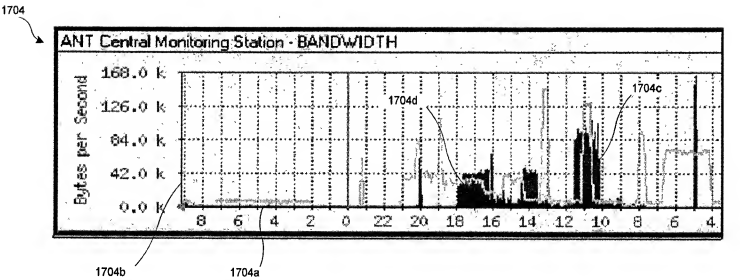
1704
ANT Central Monitoring Station - BANDWIDTH
Bytes per Second
168.0 k
126.0 k
84.0 k
42.0 k
0.0 k
8 6 4 2 0 22 20 18 16 14 12 10 8 6 4
1704d
1704c
1704b
1704a

Figure 35

1702

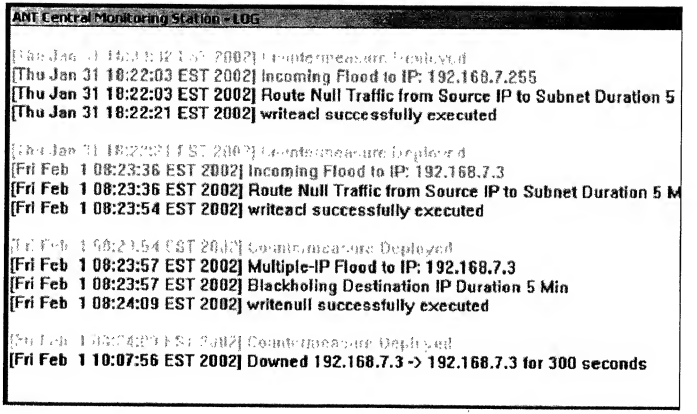

Figure 36

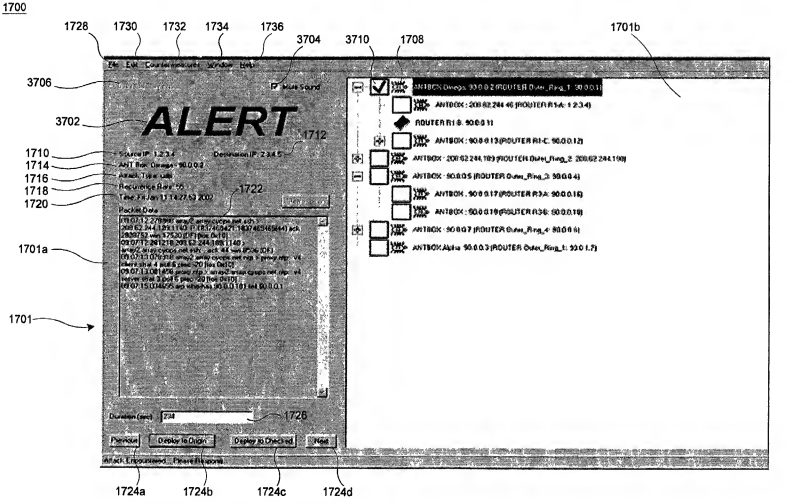
1700
1728
1730
1732
1734
1736
3704
3710
1708
1701b
3706
3702
1712
1710
1714
1716
1718
1720
1722
1701a
1701
1726
1724a
1724b
1724c
1724d
ALERT
Play Alert Sound
Previous
Display In Order
Display In Chronol
Next

Figure 37

208220" 2019800T

Figure 38

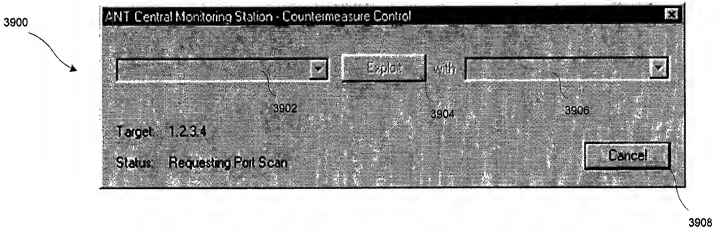
3900
ANT Central Monitoring Station - Countermeasure Control
Explor
with
3902
3904
3906
Target: 1.2.3.4
Status: Requesting Port Scan
Cancel
3908

Figure 39

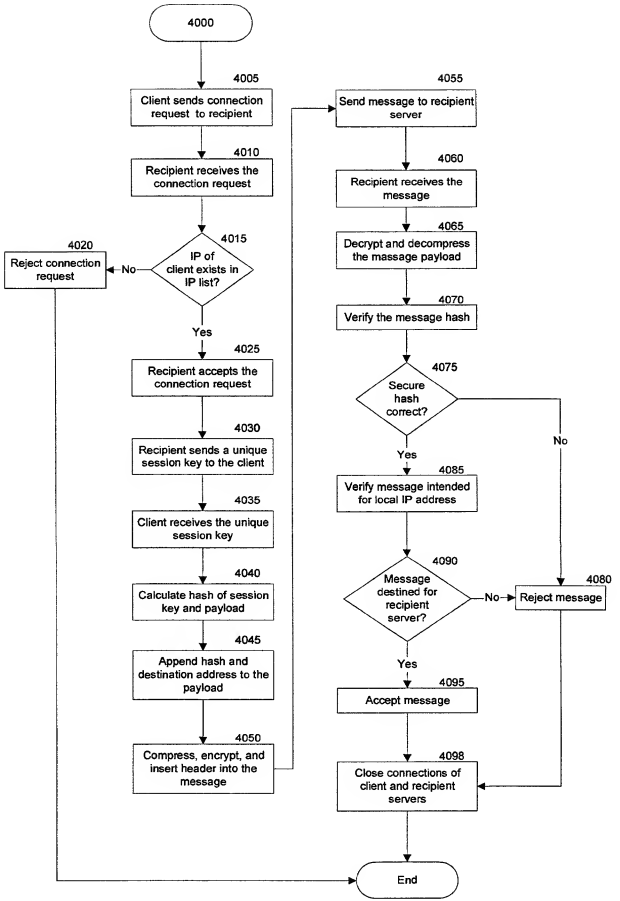

Figure 40

20020107.0228202